EXHIBIT 3

Back to Google Cloud Terms Directory (/product-terms) > Current

Cloud Data Processing Addendum (Customers)

This Cloud Data Processing Addendum (including its appendices, the "*Addendum*") is incorporated into the Agreement(s) (as defined below) between Google and Customer. This Addendum was formerly known as the "Data Processing and Security Terms" under an Agreement for Google Cloud Platform, Looker (original), Google SecOps Services, or Google Cloud Skills Boost for Organizations; the "Data Processing Amendment" under an Agreement for Google Workspace or Cloud Identity; and the "Data Processing Addendum" under an Agreement for Mandiant Consulting Services and Managed Services.

Collapse all

General Terms

1. Overview

This Addendum describes the parties' obligations, including under applicable privacy, data security, and data protection laws, with respect to the processing and security of Customer Data (as defined below). This Addendum will be effective on the Addendum Effective Date (as defined below), and will replace any terms previously applicable to the processing and security of Customer Data. Capitalized terms used but not defined in this Addendum have the meaning given to them in the Agreement.

2. Definitions

2.1 In this Addendum:

- "*Addendum Effective Date*" means the date on which Customer accepted, or the parties otherwise agreed to, this Addendum.
- "*Additional Security Controls*" means security resources, features, functionality, and controls that Customer may use at its option and as it determines, including the Admin Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.
- "*Agreement*" means the contract under which Google has agreed to provide the applicable Services to Customer.
- "*Applicable Privacy Law*" means, as applicable to the processing of Customer Personal Data, any national, federal, European Union, state, provincial or other privacy, data security, or data protection law or regulation.
- "*Audited Services*" means the then-current Services indicated as being in-scope for the relevant certification or report at https://cloud.google.com/security/compliance/services-in-scope (https://cloud.google.com/security/compliance/services-in-scope). Google may not remove any Services from this URL unless they have been discontinued in accordance with the applicable Agreement.
- "*Compliance Certifications*" has the meaning given in Section 7.4 (Compliance Certifications and SOC Reports).
- "*Customer Data*", if not defined in the Agreement, has the meaning given in Appendix 4 (Specific Products).
- "*Customer Personal Data*" means the personal data contained within the Customer Data, including any special categories of personal data or sensitive data defined under Applicable Privacy Law.
- "*Data Incident*" means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Google.
- "*EMEA*" means Europe, the Middle East and Africa.

- "*EU GDPR*" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- "*European Data Protection Law*" means, as applicable: (a) the GDPR; or (b) the Swiss FADP.
- "*European Law*" means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data); or (c) the law of Switzerland (if the Swiss FADP applies to the processing of Customer Personal Data).
- "*GDPR*" means, as applicable: (a) the EU GDPR; or (b) the UK GDPR.
- "*Google's Third-Party Auditor*" means a Google-appointed, qualified and independent third-party auditor, whose then-current identity Google will disclose to Customer.
- "*Instructions*" has the meaning given in Section 5.2 (Compliance with Customer's Instructions).
- "*Notification Email Address*" means the email address(es) designated by Customer in the Admin Console or Order Form to receive certain notifications from Google.
- "*Security Documentation*" means the Compliance Certifications and the SOC Reports.
- "*Security Measures*" has the meaning given in Section 7.1.1 (Google's Security Measures).
- "*Services*" means the applicable services described in Appendix 4 (Specific Products).
- "*SOC Reports*" has the meaning given in Section 7.4 (Compliance Certifications and SOC Reports).
- "*Subprocessor*" means a third party authorized as another processor under this Addendum to process Customer Data in order to provide parts of the Services and TSS (if applicable).

- "*Supervisory Authority*" means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; or (b) the "Commissioner" as defined in the UK GDPR or the Swiss FADP.

- "*Swiss FADP*" means, as applicable, the Federal Act on Data Protection of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 14 June 1993) or the revised Federal Act on Data Protection of 25 September 2020 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 31 August 2022).

- "*Term*" means the period from the Addendum Effective Date until the end of Google's provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Google may continue providing the Services for transitional purposes.

- "*UK GDPR*" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

2.2 The terms "personal data", "data subject", "processing", "controller", and "processor" as used in this Addendum have the meanings given by Applicable Privacy Law or, absent any such meaning or law, by the EU GDPR.

2.3 The terms "data subject", "controller" and "processor" include "consumer", "business", and "service provider", respectively, as required by Applicable Privacy Law.

3. Duration

Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, Google deletes all Customer Data as described in this Addendum.

4. Roles; Legal Compliance

4.1 *Roles of Parties.* Google is a processor and Customer is a controller or processor, as applicable, of Customer Personal Data.

4.2 *Processing Summary.* The subject matter and details of the processing of Customer Personal Data are described in Appendix 1 (Subject Matter and Details of Data Processing).

4.3 *Compliance with Law*. Each party will comply with its obligations related to the processing of Customer Personal Data under Applicable Privacy Law.

4.4 *Additional Legal Terms*. To the extent the processing of Customer Personal Data is subject to an Applicable Privacy Law described in Appendix 3 (Specific Privacy Laws), the corresponding terms in Appendix 3 will apply in addition to these General Terms and prevail as described in Section 14.1 (Precedence).

5. Data Processing

5.1 *Processor Customers*. If Customer is a processor:

a. Customer warrants on an ongoing basis that the relevant controller has authorized:

i. the Instructions;

ii. Customer's engagement of Google as another processor; and.

iii. Google's engagement of Subprocessors as described in Section 11 (Subprocessors);

b. Customer will forward to the relevant controller promptly and without undue delay any notice provided by Google under Section 7.2.1 (Incident Notification), 9.2.1 (Responsibility for Requests), or 11.4 (Opportunity to Object to Subprocessors); and

c. Customer may make available to the relevant controller any other information made available by Google under this Addendum about the locations of Google data centers or the names, locations and activities of Subprocessors.

5.2 *Compliance with Customer's Instructions*. Customer instructs Google to process Customer Data in accordance with the applicable Agreement (including this Addendum) only as follows:

a. to provide, secure, and monitor the Services and TSS (if applicable); and

b. as further specified via:

i. Customer's use of the Services (including via the Admin Console) and TSS (if applicable); and

ii. any other written instructions given by Customer and acknowledged by Google as constituting instructions under this Addendum

(collectively, the "*Instructions*").

Google will comply with the Instructions unless prohibited by European Law, where European Data Protection Law applies, or prohibited by applicable law, where any other Applicable Privacy Law applies.

6. Data Deletion

6.1 *Deletion by Customer*. Google will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an Instruction to Google to delete the relevant Customer Data from Google's systems. Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.

6.2 *Return or Deletion When Term Ends*. If Customer wishes to retain any Customer Data after the end of the Term, it may instruct Google in accordance with Section 9.1 (Access; Rectification; Restricted Processing; Portability) to return that data during the Term. Subject to Section 6.3 (Deferred Deletion Instruction), Customer instructs Google to delete all remaining Customer Data (including existing copies) from Google's systems at the end of the Term. After a recovery period of up to 30 days from that date, Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.

6.3. *Deferred Deletion Instruction*. To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Return or Deletion When Term Ends) is also processed, when the applicable Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will take effect with respect to such Customer Data only when the continuing Term expires. For clarity, this Addendum will continue to apply to such Customer Data until its deletion by Google.

7. Data Security

7.1 *Google's Security Measures, Controls and Assistance*.

7.1.1 *Google's Security Measures*. Google will implement and maintain technical, organizational, and physical measures to protect Customer Data against accidental or

unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (Security Measures) **(**the **"*Security Measures*")**. The Security Measures include measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness. Google may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services.

7.1.2 *Access and Compliance*. Google will:

a. authorize its employees, contractors and Subprocessors to access Customer Data only as strictly necessary to comply with Instructions;

b. take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance; and

c. ensure that all persons authorized to process Customer Data are under an obligation of confidentiality.

7.1.3 *Additional Security Controls*. Google will make Additional Security Controls available to:

a. allow Customer to take steps to secure Customer Data; and

b. provide Customer with information about securing, accessing and using Customer Data.

7.1.4 *Google's Security Assistance*. Google will (taking into account the nature of the processing of Customer Personal Data and the information available to Google) assist Customer in ensuring compliance with its (or, where Customer is a processor, the relevant controller's) obligations relating to security and personal data breaches under Applicable Privacy Law, by:

a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);

b. making Additional Security Controls available in accordance with Section 7.1.3 (Additional Security Controls);

c. complying with the terms of Section 7.2 (Data Incidents);

d. making the Security Documentation available in accordance with Section 7.5.1 (Reviews of Security Documentation) and providing the information contained in the applicable Agreement (including this Addendum); and

e. if subsections (a)-(d) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

7.2 *Data Incidents*.

7.2.1 *Incident Notification*. Google will notify Customer promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2 *Details of Data Incident*. Google's notification of a Data Incident will describe: the nature of the Data Incident including the Customer resources impacted; the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Google recommends that Customer take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, Google's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

7.2.3 *No Assessment of Customer Data by Google*. Google has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

7.2.4 *No Acknowledgement of Fault by Google*. Google's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

7.3 *Customer's Security Responsibilities and Assessment*.

7.3.1 *Customer's Security Responsibilities*. Without prejudice to Google's obligations under Sections 7.1 (Google's Security Measures, Controls and Assistance) and 7.2 (Data Incidents), and elsewhere in the applicable Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Google's or Google's Subprocessors' systems, including:

a. using the Services and Additional Security Controls to ensure a level of security appropriate to the risk to the Customer Data;

b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and

c. backing up or retaining copies of its Customer Data as appropriate.

7.3.2 *Customer's Security Assessment*. Customer agrees that the Services, Security Measures, Additional Security Controls, and Google's commitments under this Section 7 (Data Security) provide a level of security appropriate to the risk to Customer Data (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Data as well as the risks to individuals).

7.4 *Compliance Certifications and SOC Reports*. Google will maintain at least the following for the Audited Services to verify the continued effectiveness of the Security Measures:

a. certificates for ISO 27001 and any additional certifications described in Appendix 4 (Specific Products) (the "*Compliance Certifications*"); and

b. SOC 2 and SOC 3 reports produced by Google's Third-Party Auditor and updated annually based on an audit performed at least once every 12 months (the "*SOC Reports*").

Google may add standards at any time. Google may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

7.5 *Reviews and Audits of Compliance*.

7.5.1 *Reviews of Security Documentation*. To demonstrate compliance by Google with its obligations under this Addendum, Google will make the Security Documentation available for review by Customer and, if Customer is a processor, allow Customer to request access to the SOC Reports for the relevant controller in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

7.5.2 *Customer's Audit Rights*.

a. *Customer Audit*. Google will, if required under Applicable Privacy Law, allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under this Addendum in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). During an audit, Google will reasonably cooperate with Customer or its auditor as described in this Section 7.5 (Reviews and Audits of Compliance).

b. *Customer Independent Review*. Customer may conduct an audit to verify Google's compliance with its obligations under this Addendum by reviewing the Security Documentation (which reflects the outcome of audits conducted by Google's Third-Party Auditor).

7.5.3 *Additional Business Terms for Reviews and Audits*.

a. Customer must contact Google's Cloud Data Protection Team to request:

i. access to the SOC Reports for a relevant controller under Section 7.5.1 (Reviews of Security Documentation); or

ii. an audit under Section 7.5.2(a) (Customer Audit).

b. Following a Customer request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on:

i. security and confidentiality controls applicable to any access to the SOC Reports by a relevant controller under Section 7.5.1 (Reviews of Security Documentation); and

ii. the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2(a) (Customer Audit).

c. Google may charge a fee (based on Google's reasonable costs) for any audit under Section 7.5.2(a) (Customer Audit). Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

d. Google may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2(a) (Customer Audit) if the auditor is, in Google's reasonable opinion, not suitably qualified or independent, a competitor of Google, or otherwise manifestly unsuitable. Any such objection by Google will require Customer to appoint another auditor or conduct the audit itself.

e. Any Customer requests under Appendix 3 (Specific Privacy Laws) or Appendix 4 (Specific Products) for access to any SOC reports for a relevant controller or for audits will also be subject to this Section 7.5.3 (Additional Business Terms for Reviews and Audits).

8. Impact Assessments and Consultations

Google will (taking into account the nature of the processing and the information available to Google) assist Customer in ensuring compliance with its (or, where Customer is a processor, the relevant controller's) obligations relating to data protection assessments, risk assessments, prior regulatory consultations or equivalent procedures under Applicable Privacy Law, by:

a. making Additional Security Controls available in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation available in accordance with Section 7.5.1 (Reviews of Security Documentation);

b. providing the information contained in the applicable Agreement (including this Addendum); and

c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

9. Access; Data Subject Rights; Data Export

9.1 *Access; Rectification; Restricted Processing; Portability*. During the Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion by Customer), and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by Applicable Privacy Law.

9.2 *Data Subject Requests*.

9.2.1 *Responsibility for Requests*. During the Term, if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will:

a. advise the data subject to submit their request to Customer;

b. promptly notify Customer; and

c. not otherwise respond to that data subject's request without authorization from Customer.

Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2 *Google's Data Subject Request Assistance*. Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its (or, where Customer is a processor, the relevant controller's) obligations under Applicable Privacy Law to respond to requests for exercising the data subject's rights by:

a. making Additional Security Controls available in accordance with Section 7.1.3 (Additional Security Controls);

b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); and

c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

10. Data Processing Locations

10.1 *Data Storage and Processing Facilities*. Subject to Google's data location commitments under the Service Specific Terms and data transfer commitments under Appendix 3 (Specific Privacy Laws), if applicable, Customer Data may be processed in any country where Google or its Subprocessors maintain facilities.

10.2 *Data Center Information*. The locations of Google data centers are described in Appendix 4 (Specific Products).

11. Subprocessors

11.1 *Consent to Subprocessor Engagement*. Customer specifically authorizes Google's engagement as Subprocessors of those entities disclosed as described in Section 11.2 (Information about Subprocessors) as of the Addendum Effective Date. In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessors), Customer generally authorizes Google's engagement of other third parties as Subprocessors ("*New Subprocessors*").

11.2 *Information about Subprocessors*. Names, locations, and activities of Subprocessors are described in Appendix 4 (Specific Products).

11.3 *Requirements for Subprocessor Engagement*. When engaging any Subprocessor, Google will:

a. ensure via a written contract that:

i. the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Addendum); and

ii. if required under Applicable Privacy Laws, the data protection obligations described in this Addendum are imposed on the Subprocessor (as may be further described in Appendix 3 (Specific Privacy Laws)); and

b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 *Opportunity to Object to Subprocessors*.

a. When Google engages any New Subprocessor during the Term, Google will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name, location and activities of the New Subprocessor).

b. Customer may, within 90 days after being notified of the engagement of a New Subprocessor, object by immediately terminating the applicable Agreement for convenience:

i. in accordance with that Agreement's termination for convenience provision; or

ii. if there is no such provision, by notifying Google.

12. Cloud Data Protection Team; Processing Records

12.1 *Cloud Data Protection Team*. Google's Cloud Data Protection Team will provide prompt and reasonable assistance with any Customer queries related to processing of Customer Data under the applicable Agreement and can be contacted as described in the Notices section of the applicable Agreement or in Appendix 4 (Specific Products).

12.2 *Google's Processing Records*. Google will keep appropriate documentation of its processing activities as required by Applicable Privacy Law. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will use the Admin Console or other means identified in Appendix 4

(Specific Products) to supply such information and keep it accurate and up-to-date. Google may make any such information available to competent regulators, including a Supervisory Authority, if required by Applicable Privacy Law.

12.3 *Controller Requests*. During the Term, if Google's Cloud Data Protection Team receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Google will advise the third party to contact Customer.

13. Notices

Notices under this Addendum (including notifications of any Data Incidents) will be delivered to the Notification Email Address. Customer is responsible for using the Admin Console, or otherwise notifying Google, to ensure that its Notification Email Address remains current and valid.

14. Interpretation

14.1 *Precedence*. To the extent of any conflict between:

a. Appendix 3 (Specific Privacy Laws) and the remainder of the Addendum (including Appendix 4 (Specific Products)), Appendix 3 will prevail; and

b. Appendix 4 (Specific Products) and the remainder of the Addendum (excluding Appendix 3), Appendix 4 will prevail; and

c. this Addendum and the remainder of the Agreement, this Addendum will prevail.

For clarity, if Customer has more than one Agreement, this Addendum will amend each of the Agreements separately.

14.2 *Section References*. Unless indicated otherwise, section references in any Appendix to this Addendum refer to sections of the General Terms of the Addendum.

Appendix 1: Subject Matter and Details of Data Processing

Subject Matter

Google's provision of the Services and TSS (if applicable) to Customer.

Duration of the Processing

The Term plus the period from the end of the Term until deletion of all Customer Data by Google in accordance with this Addendum.

Nature and Purpose of the Processing

Google will process Customer Personal Data for the purposes of providing the Services and TSS (if applicable) to Customer in accordance with this Addendum.

Categories of Data

Data relating to individuals provided to Google via the Services, by (or at the direction of) Customer or by its End Users.

Data Subjects

Data subjects include the individuals about whom data is provided to Google via the Services by (or at the direction of) Customer or by its End Users.

Appendix 2: Security Measures

As from the Addendum Effective Date, Google will implement and maintain the Security Measures described in this Appendix 2.

1. Data Center and Network Security

(a) Data Centers.

Infrastructure. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and

frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy.

Code Quality. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(*b) Networks and Transmission*.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves: (i) tightly controlling the size and make-up of Google's attack surface through preventative measures; (ii) employing intelligent detection controls at data entry points; and (iii) employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls

(a) Site Controls.

On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ a dual authentication access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Customer's Administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorized persons and systems from gaining access to systems used to process Customer Data. Google designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Google's authentication and authorization systems utilize SSH certificates and security keys, and are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the

use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g. credit card data), Google uses hardware tokens.

3. Data

(a) *Data Storage, Isolation and Logging*. Google stores data in a multi-tenant environment on Google-owned servers. Subject to any Instructions to the contrary (e.g. in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data. Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to its End Users for specific purposes. Customer may choose to use logging functionality that Google makes available via the Services.

(b) *Decommissioned Disks and Disk Erase Policy*. Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and

professional standards. Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Google personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g. certifications). Google's personnel will not process Customer Data without authorization.

5. Subprocessor Security

Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement), the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Appendix 3: Specific Privacy Laws

The terms in each subsection of this Appendix 3 apply only where the corresponding law applies to the processing of Customer Personal Data.

European Data Protection Law

1. Additional Definitions.

- "*Adequate Country*" means:

  (a) for data processed subject to the EU GDPR: the European Economic Area, or a country or territory recognized as ensuring adequate protection under the EU GDPR;

  (b) for data processed subject to the UK GDPR: the UK, or a country or territory recognized as ensuring adequate protection under the UK GDPR and the Data

Protection Act 2018; or

(c) for data processed subject to the Swiss FADP: Switzerland, or a country or territory that is: (i) included in the list of the states whose legislation ensures adequate protection as published by the Swiss Federal Data Protection and Information Commissioner, if applicable; or (ii) recognized as ensuring adequate protection by the Swiss Federal Council under the Swiss FADP;

in each case, other than on the basis of an optional data protection framework.

- "*Alternative Transfer Solution*" means a solution, other than SCCs, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law, for example a data protection framework recognized as ensuring that participating entities provide adequate protection.
- "*Customer SCCs*" means the SCCs (Controller-to-Processor), the SCCs (Processor-to-Processor), or the SCCs (Processor-to-Controller), as applicable.
- "*SCCs*" means the Customer SCCs or SCCs (Processor-to-Processor, Google Exporter), as applicable.
- "*SCCs (Controller-to-Processor)*" means the terms at: https://cloud.google.com/terms/sccs/eu-c2p (https://cloud.google.com/terms/sccs/eu-c2p)
- "*SCCs (Processor-to-Controller)*" means the terms at: https://cloud.google.com/terms/sccs/eu-p2c (https://cloud.google.com/terms/sccs/eu-p2c)
- "*SCCs (Processor-to-Processor)*" means the terms at: https://cloud.google.com/terms/sccs/eu-p2p (https://cloud.google.com/terms/sccs/eu-p2p)
- "*SCCs (Processor-to-Processor, Google Exporter)*" means the terms at: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter (https://cloud.google.com/terms/sccs/eu-p2p-google-exporter)

2. Instruction Notifications. Without prejudice to Google's obligations under Section 5.2 (Compliance with Customer's Instructions) or any other rights or obligations of either party under the applicable Agreement, Google will immediately notify Customer if, in Google's opinion:

a. European Law prohibits Google from complying with an Instruction;

b. an Instruction does not comply with European Data Protection Law; or

c. Google is otherwise unable to comply with an Instruction,

in each case unless such notice is prohibited by European Law.

If Customer is a processor, Customer will immediately forward to the relevant controller any notice provided by Google under this section.

3. Customer's Audit Rights. Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) as described in Section 7.5.2(a) (Customer Audit). During such an audit, Google will make available all information necessary to demonstrate compliance with its obligations under this Addendum and contribute to the audit as described in Section 7.5 (Reviews and Audits of Compliance) and this section.

4. Data Transfers.

4.1 *Restricted Transfers*. The parties acknowledge that European Data Protection Law does not require SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country. If Customer Personal Data is transferred to any other country and European Data Protection Law applies to the transfers (as certified by Customer under Section 4.2 (Certification by Non-EMEA Customers) of these European Data Protection Law terms, if its billing address is outside EMEA) ("*Restricted Transfers*"), then:

a. if Google has adopted an Alternative Transfer Solution for any Restricted Transfers, Google will inform Customer of the relevant solution and ensure that such Restricted Transfers are made in accordance with it; or

b. if Google has not adopted an Alternative Transfer Solution for any Restricted Transfers, or informs Customer that Google is no longer adopting, an Alternative Transfer Solution for any Restricted Transfers (without adopting a replacement Alternative Transfer Solution):

i. if Google's address is in an Adequate Country:

A. the SCCs (Processor-to-Processor, Google Exporter) will apply with respect to such Restricted Transfers from Google to Subprocessors; and

B. in addition, if Customer's billing address is not in an Adequate Country, the SCCs (Processor-to Controller) will apply (regardless of whether Customer is a controller or processor) with respect to such Restricted Transfers between Google and Customer; or

ii. if Google's address is not in an Adequate Country, the SCCs (Controller-to-Processor) or SCCs (Processor-to-Processor) will apply (according to whether Customer is a controller or processor) with respect to such Restricted Transfers between Google and Customer.

4.2 *Certification by Non-EMEA Customers*. If Customer's billing address is outside EMEA, and the processing of Customer Personal Data is subject to European Data Protection Law, then unless Appendix 4 (Specific Products) of this Addendum indicates otherwise, Customer will certify as such and identify its competent Supervisory Authority via the Admin Console for the applicable Services.

4.3 *Information about Restricted Transfers*. Google will provide Customer with information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures:

a. as described in Section 7.5.1 (Reviews of Security Documentation);

b. in any additional locations described in Appendix 4 (Specific Products); and

c. in relation to Google's adoption of an Alternative Transfer Solution, at https://cloud.google.com/terms/alternative-transfer-solution (https://cloud.google.com/terms/alternative-transfer-solution).

4.4 *SCC Audits*. If Customer SCCs apply as described in Section 4.1 (Restricted Transfers) of these European Data Protection Law terms, Google will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs, both in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

4.5 *SCC Notices*. Customer will forward to the relevant controller promptly and without undue delay any notice that refers to any SCCs.

4.6 *Termination Due to Data Transfer Risk*. If Customer concludes, based on its current or intended use of the Services, that appropriate safeguards are not provided for transferred Customer Personal Data, then Customer may immediately terminate the applicable

Agreement in accordance with that Agreement's termination for convenience provision or, if there is no such provision, by notifying Google.

4.7 *No Modification of SCCs*. Nothing in the Agreement (including this Addendum) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

4.8 *Precedence of SCCs*. To the extent of any conflict or inconsistency between any Customer SCCs (which are incorporated by reference into this Addendum) and the remainder of the Agreement (including this Addendum), the Customer SCCs will prevail.

5. Requirements for Subprocessor Engagement. European Data Protection Law requires Google to ensure via a written contract that the data protection obligations described in this Addendum, as referred to in Article 28(3) of the GDPR, if applicable, are imposed on any Subprocessor engaged by Google.

CCPA

1. Additional Definitions.

- "*CCPA*" means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.
- "*Customer Personal Data*" includes "personal information".
- The terms "business", "business purpose", "consumer", "personal information", "processing", "sale", "sell", "service provider", and "share" have the meanings given in the CCPA.

2. Prohibitions. Without prejudice to Google's obligations under Section 5.2 (Compliance with Customer's Instructions), with respect to the processing of Customer Personal Data in accordance with the CCPA, Google will not, unless otherwise permitted under the CCPA:

a. sell or share Customer Personal Data;

b. retain, use or disclose Customer Personal Data:

i. other than for a business purpose under the CCPA on behalf of Customer and for the specific purpose of performing the Services and TSS (if applicable); or

ii. outside of the direct business relationship between Google and Customer; or

c. combine or update Customer Personal Data with personal information that Google receives from or on behalf of a third party or collects from its own interactions with the consumer.

3. Compliance. Without prejudice to Google's obligations under Section 5.2 (Compliance with Customer's Instructions) or any other rights or obligations of either party under the applicable Agreement, Google will notify Customer if, in Google's opinion, Google is unable to meet its obligations under the CCPA, unless such notice is prohibited by applicable law.

4. Customer Intervention. If Google notifies Customer of any unauthorized use of Customer Personal Data, including under Section 3 (Compliance) of this subsection or Section 7.2.1 (Incident Notification), Customer may take reasonable and appropriate steps to stop or remediate such unauthorized use by:

a. taking any measures recommended by Google pursuant to Section 7.2.2 (Details of Data Incident), if applicable; or

b. exercising its rights under Section 7.5.2(a) (Customer Audit) or 9.1 (Access; Rectification; Restricted Processing; Portability).

Turkey

1. Additional Definitions.

- "*Turkish Data Protection Law*" means the Turkish Law on the Protection of Personal Data No. 6698 dated April 7, 2016.
- "*Turkish Personal Data Protection Authority*" means the Kişisel Verileri Koruma Kurumu.
- "*Turkish SCCs*" means standard contract clauses under Turkish Data Protection Law.

2. Data Transfers.

2.1 *Supplementary Terms*. If Customer's billing address is in Turkey and Google makes any optional additional terms (including Turkish SCCs) available for acceptance by Customer in relation to transfers of Customer Personal Data under Turkish Data Protection Law, those terms will supplement this Addendum as from the date they are notified to the Turkish Personal Data Protection Authority in accordance with Section 2.2 (Notification to the Competent Authority) below, as evidenced by Customer to Google.

2.2 *Notification to the Competent Authority*. If Customer enters into Turkish SCCs under this Section 2 (Data Transfers), Customer will be responsible for notifying the Turkish Personal Data Protection Authority of use of Turkish SCCs within five (5) business days of signature of the Turkish SCCs as required by Turkish Data Protection Law.

2.3 *SCC Audits*. If Customer enters into Turkish SCCs under this Section 2 (Data Transfers), Google will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs, both in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

2.4 *Termination Due to Data Transfer Risk*. If Customer concludes, based on its current or intended use of the Services, that appropriate safeguards are not provided for transferred Customer Personal Data, then Customer may immediately terminate the applicable Agreement in accordance with that Agreement's termination for convenience provision or, if there is no such provision, by notifying Google.

2.5 *No Modification of Turkish SCCs*. Nothing in the Agreement (including this Addendum) is intended to modify or contradict the Turkish SCCs or prejudice the fundamental rights or freedoms of data subjects under Turkish Data Protection Law.

2.6 *Precedence of SCCs*. To the extent of any conflict or inconsistency between the Turkish SCCs (which will be incorporated by reference into this Addendum if entered into by Customer) and the remainder of the Agreement (including this Addendum), the Turkish SCCs will prevail.

Israel

1. Additional Definition.

- "*Israeli Privacy Protection Law*" means the Israeli Privacy Protection Law, 1981 and any regulations promulgated thereunder.

2. Equivalent Terms. Any terms equivalent to "controller", "personal data", "processing", and "processor", as used in this Addendum, have the meanings given in the Israeli Privacy Protection Law.

3. Customer's Audit Rights. Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) as described in Section 7.5.2(a) (Customer Audit).

Appendix 4: Specific Products

The terms in each subsection of this Appendix 4 apply solely with respect to the processing of Customer Data by the corresponding Service(s).

Google Cloud Platform

1. Additional Definitions.

- "*Account*", if not defined in the Agreement, means Customer's Google Cloud Platform account.
- "*Customer Data*", if not defined in the Agreement, means data provided to Google by Customer or End Users through Google Cloud Platform under the Account, and data that Customer or End Users derive from that data through their use of Google Cloud Platform.
- "*Google Cloud Platform*" means the Google Cloud Platform services described at https://cloud.google.com/terms/services (https://cloud.google.com/terms/services), excluding any Third-Party Offerings.
- "*Third-Party Offerings*", if not defined in the Agreement, means (a) third-party services, software, products, and other offerings that are not incorporated into Google Cloud Platform or Software, (b) offerings identified in the "Third-Party Terms" section of the Service Specific Terms of the Agreement, and (c) third-party operating systems.

2. Compliance Certifications. The Compliance Certifications for Google Cloud Platform Audited Services will also include certificates for ISO 27017 and ISO 27018 and a PCI DSS Attestation of Compliance.

3. Data Center Locations. The locations of Google Cloud Platform data centers are described at https://cloud.google.com/about/locations/ (https://cloud.google.com/about/locations/).

4. Information about Subprocessors. Names, locations, and activities of Google Cloud Platform Subprocessors are described at https://cloud.google.com/terms/subprocessors (https://cloud.google.com/terms/third-party-suppliers).

5. Cloud Data Protection Team. The Data Protection Team for Google Cloud Platform can be contacted at https://support.google.com/cloud/contact/dpo (https://support.google.com/cloud/contact/dpo).

6. Information about Restricted Transfers. Additional information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures is available at cloud.google.com/privacy/ (https://cloud.google.com/privacy).

7. Service Specific Terms.

Bare Metal Solution (Google Cloud Platform)

Bare Metal Solution provides non-virtualized access to underlying infrastructure resources and, by design, has certain distinct characteristics.

1. Amendments. This Addendum is amended as follows with respect to Bare Metal Solution:

- The definition of "Google's Third-Party Auditor" is replaced with the following:
    - "*Google's Third-Party Auditor*" means a qualified and independent third-party auditor appointed by Google or a Bare Metal Solution Subprocessor, whose then-current identity Google will disclose to Customer on request.
- The following terms are deleted:
    - From Section 7.1.1 (Google's Security Measures), the phrase "Encrypt Customer Data";
    - From Appendix 2 (Security Measures), the Section 1(a) subsections titled "Server Operating Systems" and "Business Continuity";
    - From Appendix 2, the Section 1(b) subsections titled "External Attack Surface," "Intrusion Detection," and "Encryption Technologies"; and
    - From Appendix 2, the following sentences of Section 3(a):
        - Google stores data in a multi-tenant environment on Google-owned servers. Subject to any Customer instructions to the contrary (for example, in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers.

2. Compliance Certifications and SOC Reports. Google or its Subprocessor will maintain at least the following (or an equivalent or enhanced alternative) for Bare Metal Solution to verify the continued effectiveness of the Security Measures:

a. a certificate for ISO 27001 and a PCI DSS Attestation of Compliance (the "*BMS Compliance Certifications*"); and

b. SOC 1 and SOC 2 reports updated annually based on an audit performed at least once every 12 months (the "*BMS SOC Reports*").

3. Reviews of Security Documentation. To demonstrate compliance by Google with its obligations under this Addendum, Google will make the BMS Compliance Certifications and BMS SOC Reports available for review by Customer and, if Customer is a processor, allow Customer to request access for the relevant controller to the BMS SOC Reports in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

4. Customer Obligations. Without limiting Google's express obligations related to Bare Metal Solution, Customer will take reasonable steps to protect and maintain the security of Customer Data and any other content stored on or processed through Bare Metal Solution.

5. Disclaimer. Notwithstanding anything to the contrary in the Agreement (including this Addendum), Google is not responsible for any of the following in relation to Bare Metal Solution:

a. non-physical security, such as access controls, encryption, firewalls, antivirus protection, threat detection, and security scanning;

b. logging and monitoring;

c. non-hardware maintenance or support;

d. data backup, including any redundancy or high-availability configuration; or

e. business continuity and disaster recovery policies or procedures.

Customer is solely responsible for securing (other than physical security of Bare Metal Solution servers), logging and monitoring, maintaining and supporting, and backing up any Operating Systems, Customer Data, software, and applications Customer uses with, uploads to, or hosts on Bare Metal Solution.

Cloud NGFW (Google Cloud Platform)

The edition of Cloud NGFW titled "Cloud NGFW Enterprise" ("CNE") is designed to mitigate cybersecurity risks and, as such, has certain distinct characteristics.

1. Amendments. The Addendum is amended as follows with respect to CNE:

- Sections 6.1 (Deletion by Customer) and 6.2 (Return or Deletion When Term Ends) will not prevent Google or Subprocessors from retaining any file or network traffic packet capture submitted for TSS purposes and designated by CNE as a security threat, provided that the file or network traffic packet capture does not include Customer Personal Data.

Google Distributed Cloud connected (Google Cloud Platform)

Google Distributed Cloud connected is not deployed at a Google data center and, by design, has certain distinct characteristics.

1. Amendments. This Addendum is amended as follows with respect to Google Distributed Cloud connected:

- References to "Google's systems" are replaced with "the Equipment."
- Section 6.2 (Return or Deletion When Term Ends) is replaced with the following:
    - 6.2 *Return or Deletion at the end of the Term*. Customer instructs Google to delete all remaining Customer Data (including existing copies) from the Equipment at the end of the Term in accordance with applicable law. If Customer wishes to retain any Customer Data after the end of the Term, it may export or make copies of such data prior to the end of the Term. Google will comply with the Instruction in this Section 6.2 as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.
- The following words are added to the end of Section 10.1 (Data Storage and Processing Facilities): "or where the Customer Location is located."
- Section 1 (Data Center and Network Security) of Appendix 2 (Security Measures) is replaced with the following:
    - **1. Local Machines and Network Security**

Local Machines. Customer Data is solely stored on the Equipment to be deployed in a Customer Location.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Google employs a code review process to increase the security of the code used to provide Google Distributed Cloud connected and enhance the security products in Google Distributed Cloud connected production environments.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available and allows for encryption of data in transit. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough. Google also makes encryption of data at rest available, using at least AES128 or similar. Google Distributed Cloud connected has a CMEK integration; more information can be found at https://cloud.google.com/kms/docs/cmek (https://cloud.google.com/kms/docs/cmek).

Connection to Cloud VPN. Google allows Customer to enable and configure a strong, encrypted interconnection between the Equipment and Customer's Virtual Private Cloud using Cloud VPN through an IPSEC VPN connection.

Bound Storage. Customer's data storage is bound to the server. Should a disk be stolen or copied at rest, the contents of such disk will be unrecoverable outside of the server.

- Sections 2 (Access and Site Controls) and 3 (Data) of Appendix 2 (Security Measures) are deleted.

2. Inapplicable Provisions. Any Google obligations in the Agreement (including this Addendum) or statements in associated security documentation (including whitepapers) that depend on Google's operation of a Google data center do not apply to Google Distributed Cloud connected.

Google-Managed Multi-Cloud (Google Cloud Platform)

Google-Managed Multi-Cloud Services involve third-party infrastructure and, by design, have certain distinct characteristics.

1. Additional Definition.

- "*Google-Managed MCS Data Processing Amendment*" means the terms at https://cloud.google.com/terms/mcs-data-processing-terms (https://cloud.google.com/terms/mcs-data-processing-terms).

2. Multi-Cloud Data Processing Terms. The Google-Managed MCS Data Processing Amendment supplements and amends this Addendum with respect to Google-Managed Multi-Cloud Services for Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

Google may not have access to Customer's VMware environment or be able to encrypt personal data in Customer's VMware environment.

NetApp Volumes (Google Cloud Platform)

1. Amendments. This Addendum is amended as follows with respect to NetApp Volumes:

- The definition of "Google's Third-Party Auditor" is replaced with the following:
  - "*Google's Third Party Auditor*" means a qualified and independent third party auditor appointed by Google or a NetApp Volumes Subprocessor, whose then-current identity Google will disclose to Customer on request.
- Section 3(a) (Data Storage, Isolation and Logging) of Appendix 2 (Security Measures) is replaced with the following:
  - (a) *Data Storage, Isolation and Logging*. Google stores data in a multi-tenant environment on servers owned by NetApp, Inc. Subject to any Instructions to the contrary (e.g. in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data. Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to its End Users for specific purposes. Customer may choose to use logging functionality that Google makes available via the Services.

2. Compliance Certifications and SOC Reports. Google or its Subprocessor will obtain at least the following (or an equivalent or enhanced alternative) for NetApp Volumes:

a. a certificate for ISO 27001 and a PCI DSS Attestation of Compliance (the "*NetApp Compliance Certifications*"); and

b. SOC 1 and SOC 2 Reports updated annually based on an audit performed at least once every 12 months (the "*NetApp SOC Reports*").

3. Reviews of Security Documentation. To demonstrate compliance by Google with its obligations under this Addendum, Google will make any NetApp Compliance Certifications and NetApp SOC Reports available for review by Customer and, if Customer is a processor, allow Customer to request access for the relevant controller to the NetApp SOC Reports in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

Google Workspace and Cloud Identity

1. Additional Definitions.

- "*Account*", if not defined in the Agreement, means Customer's Google Workspace or Cloud Identity account.
- "*Cloud Identity*" when purchased under a standalone Agreement and not as part of Google Cloud Platform or Google Workspace, means the Cloud Identity Services described at https://cloud.google.com/terms/identity/user-features (https://cloud.google.com/terms/identity/user-features).
- "*Customer Data*", if not defined in the Agreement, means data submitted, stored, sent or received by or on behalf of Customer or its End Users via Google Workspace or Cloud Identity under the Account.
- "*Google Workspace*" means the Google Workspace or Google Workspace for Education services described at https://workspace.google.com/terms/user_features.html (https://workspace.google.com/terms/user_features.html), as applicable.

2. Additional Products. If Google at its option makes Additional Products available to Customer for use with Google Workspace or Cloud Identity in accordance with applicable Additional Product Terms:

a. Customer may enable or disable Additional Products via the Admin Console and will not need to use Additional Products in order to use Google Workspace or Cloud Identity; and

b. if Customer opts to install any Additional Products or to use them with Google Workspace or Cloud Identity, the Additional Products may access Customer Data as required to interoperate with Google Workspace or Cloud Identity, as applicable.

For clarity, this Addendum does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products.

3. Compliance Certifications. The Compliance Certifications for Google Workspace and Cloud Identity Audited Services will also include certificates for ISO 27017 and ISO 27018.

4. Data Center Locations. The locations of Google Workspace and Cloud Identity data centers are described at https://www.google.com/about/datacenters/locations/ (https://www.google.com/about/datacenters/locations/).

5. Information about Subprocessors. Names, locations, and activities of Google Workspace and Cloud Identity Subprocessors are described at https://workspace.google.com/intl/en/terms/subprocessors.html (https://workspace.google.com/intl/en/terms/subprocessors.html).

6. Cloud Data Protection Team. The Data Protection Team for Google Workspace and Cloud Identity (while Administrators are signed in to their Admin Account) can be contacted at https://support.google.com/a/contact/googlecloud_dpr (https://support.google.com/a/contact/googlecloud_dpr).

7. Additional Security Measures. For Google Workspace and Cloud Identity:

a. Google logically separates each End User's data from the data of other End Users; and

b. data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared).

8. Information about Restricted Transfers. Additional information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures is available at cloud.google.com/privacy/ (https://cloud.google.com/privacy).

9. Service Data Addendum. If Google makes an optional Service Data Addendum available for acceptance by Customer in relation to this Addendum, availability of that optional addendum will constitute a "DPA Update" if such term is defined in any Service Data Addendum previously entered into by Customer.

10. Service Specific Terms.

AppSheet (Google Workspace)

1. Amendments. This Addendum is amended as follows with respect to AppSheet:

- The paragraph titled "Server Operating Systems" in Section 1(a) of Appendix 2 (Security Measures) is replaced with the following:
    - *Server Operating Systems*. Google servers use a Linux based implementation customized for the application environment.

2. Additional Data Center Locations. Additional data center locations for AppSheet are described at https://cloud.google.com/about/locations/ (https://cloud.google.com/about/locations/).

Looker (original)

1. Additional Definitions.

- "*Admin Console*" means any admin console applicable to each Instance.
- "*Google-Managed MCS Data Processing Amendment*" means, if applicable, the terms at https://cloud.google.com/terms/mcs-data-processing-terms (https://cloud.google.com/terms/mcs-data-processing-terms).
- "*Google-Managed Multi-Cloud Services*" means, if applicable, specified Google services, products and features that are hosted on the infrastructure of a third party cloud provider.
- "*Looker (original)*" means an integrated platform (including cloud-based infrastructure, if applicable, and software components including any associated APIs) that enables businesses to analyze data and define business metrics across multiple data sources made available by Google to Customer under the Agreement. Looker (original) excludes Third-Party Offerings.
- "*Multi-Cloud Service Third-Party Provider*" has the meaning given in the Google-Managed MCS Data Processing Amendment.
- "*Order Form*" has the meaning given in the Agreement, unless Customer has purchased via a reseller or online marketplace or is using Looker only for trial or evaluation purposes under a trial or evaluation agreement, in which case Order Form

may mean another written form (email or other electronic means permitted) as authorized by Google.

2. Amendments. This Addendum is amended as follows with respect to Looker (original):

- The definition of "Notification Email Address" is replaced with the following:
  - "Notification Email Address" means the email address(es) designated by Customer in the Order Form or via Looker (as applicable) to receive certain notifications from Google.
- The definitions of "SCCs (Controller-to-Processor)", "SCCs (Processor-to-Controller)", "SCCs (Processor-to-Processor)" and "SCCs (Processor-to-Processor, Google Exporter)" in Appendix 3 (Specific Privacy Laws) are replaced with the following:
  - "*SCCs (Controller-to-Processor)*" means the terms at: https://cloud.google.com/terms/looker/legal/sccs/eu-c2p (https://cloud.google.com/terms/looker/legal/sccs/eu-c2p);
  - "*SCCs (Processor-to-Controller)*" means the terms at: https://cloud.google.com/terms/looker/legal/sccs/eu-p2c (https://cloud.google.com/terms/looker/legal/sccs/eu-p2c);
  - "*SCCs (Processor-to-Processor)*" means the terms at: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p (https://cloud.google.com/terms/looker/legal/sccs/eu-p2p); and
  - "*SCCs (Processor-to-Processor, Google Exporter)*" means the terms at: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group (https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group).
- The following words are added to the end of Section 10.1 (Data Storage and Processing Facilities): "or where any Multi-Cloud Service Third-Party Providers maintain facilities."

3. Additional Customer Security Responsibilities. Customer is responsible for the security of Customer's environment, databases, and configuration for Looker (original) excluding systems managed and controlled by Google.

4. Compliance Certifications and SOC Reports. The Compliance Certifications and SOC Reports for Looker (original) Audited Services may vary according to the hosting environment in which the relevant Services are used. Google will provide details of the Compliance Certifications and SOC Reports available for specific hosting environments on request.

5. Data Center Locations. The locations of Looker (original) data centers will be described on the applicable Order Form or otherwise identified by Google.

6. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for Looker (original).

7. Information about Restricted Transfers. Additional information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures for Looker (original) is available at https://docs.looker.com (https://docs.looker.com).

8. Information about Subprocessors. Names, locations and activities of Subprocessors for Looker (original) are described at:

a. https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors (https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors) and

b. https://cloud.google.com/terms/subprocessors (https://cloud.google.com/terms/subprocessors).

9. Google-Managed Multi-Cloud (Looker (original))

Google-Managed Multi-Cloud Services involve third-party infrastructure and, by design, have certain distinct characteristics.

9.1 *Multi-Cloud Data Processing Terms*. The Google-Managed MCS Data Processing Amendment supplements and amends this Addendum with respect to Google-Managed Multi-Cloud Services for Looker (original).

10. Cloud Data Protection Team. The Data Protection Team for Looker (original) can be contacted at https://support.google.com/cloud/contact/dpo (https://support.google.com/cloud/contact/dpo).

11. Google's Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

12. Additional Application Security Measures. Google will implement and maintain the additional Security Measures described below for Looker (original):

a. Google follows at least industry standard practices for security architecture. Proxy servers used for Google's applications help secure access to Looker by providing a single point to filter attacks through IP denylisting and connection rate limiting.

b. Customer administrators control access to applications by Google personnel to provide technical support requested by Customer or End Users.

SecOps Services

1. Additional Definitions.

- "*Account*", if not defined in the Agreement, means Customer's SecOps Services or Google Cloud Platform account, as applicable.
- "*Customer Data*", if not defined in the Agreement, means data provided to Google by Customer or End Users through SecOps Services under the Account or, for Mandiant Consulting Services and Managed Services, in connection with receiving SecOps Services.
- "*Customer-Engaged Provider*" means a service provider (which may include a processor or subprocessor) directly engaged by Customer under a separate agreement between Customer and such provider.
- "*SecOps Services*" means the SecOps Services described at https://cloud.google.com/terms/secops/services (https://cloud.google.com/terms/secops/services), excluding any Third-Party Offerings.
- "*Third-Party Offerings*", if not defined in the Agreement, means (a) third-party services, software, products, and other offerings that are not incorporated into SecOps Services or Software, and (b) third-party operating systems.

2. Amendments. This Addendum is amended as follows with respect to SecOps Services:

- The definition of "Additional Security Controls" is replaced with the following:
  - *"Additional Security Controls"* means security resources, features, functionality and/or controls (if any) that Customer may use at its option and/or as it determines, including (if any) encryption, logging and monitoring, identity and access management, and security scanning.
- The definition of "Audited Services" is replaced with the following:
  - "*Audited Services*" means the then-current SecOps Services indicated as being in-scope for the relevant certification or report at https://cloud.google.com/security/compliance/secops/services-in-scope (https://cloud.google.com/security/compliance/secops/services-in-scope). Google may not remove any SecOps Services from this URL unless they have been discontinued in accordance with the applicable Agreement.
- The definitions of "SCCs (Controller-to-Processor)", "SCCs (Processor-to-Controller)", "SCCs (Processor-to-Processor)" and "SCCs (Processor-to-Processor, Google Exporter)" in Appendix 3 (Specific Privacy Laws) are replaced with the following:
  - "SCCs (Controller-to-Processor)" means the terms at: https://cloud.google.com/terms/secops/sccs/eu-c2p (https://cloud.google.com/terms/secops/sccs/eu-c2p);
  - "SCCs (Processor-to-Controller)" means the terms at: https://cloud.google.com/terms/secops/sccs/eu-p2c (https://cloud.google.com/terms/secops/sccs/eu-p2c);
  - "SCCs (Processor-to-Processor)" means the terms at: https://cloud.google.com/terms/secops/sccs/eu-p2p (https://cloud.google.com/terms/secops/sccs/eu-p2p); and
  - "SCCs (Processor-to-Processor, Google Exporter)" means the terms at: https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter (https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter). (https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter)
- Section 6.1 (Deletion by Customer) is modified to read as follows:

- 6.1 **Deletion by Customer**. Google will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services or upon request. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, or if Customer requests deletion of any Customer Data during the Term, this use or request (as applicable) will constitute an Instruction to Google to delete the relevant Customer Data from Google's systems in accordance with applicable law. Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage, where European Data Protection Law applies, or applicable law requires storage, where any other Applicable Privacy Law applies.

- Section 7.4 (Compliance Certifications and SOC Reports) of the Addendum is modified to read as follows:

  - 7.4 *Compliance Certifications and SOC Reports*. Google will maintain at least the certifications and reports as identified at https://cloud.google.com/security/compliance/secops/services-in-scope (https://cloud.google.com/security/compliance/secops/services-in-scope) for the Audited Services to verify the continued effectiveness of the Security Measures (the "**Compliance Certifications**" and "**SOC Reports**").

    Google may add standards at any time. Google may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

- Section 9.1 (Access; Rectification; Restricted Processing; Portability) is modified to read as follows:

  9.1 **Access; Rectification; Restricted Processing; Portability**. During the Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including as described in Section 6.1 (Deletion by Customer), and to export Customer Data upon request. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for notifying Google and Google will assist Customer in rectifying that data if required by Applicable Privacy Law.

3. Data Center Locations. The locations of SecOps Services data centers are described at https://cloud.google.com/terms/secops/data-residency (https://cloud.google.com/terms/secops/data-residency).

4. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for SecOps Services.

5. Information about Subprocessors. Names, locations, and activities of Subprocessors for SecOps Services are described at https://cloud.google.com/terms/secops/subprocessors (https://cloud.google.com/terms/secops/subprocessors).

6. Cloud Data Protection Team. The Data Protection Team for SecOps Services can be contacted at https://support.google.com/cloud/contact/dpo (https://support.google.com/cloud/contact/dpo) (and/or via such other means as Google may provide from time to time).

7. Google's Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

8. Service Specific Terms.

Mandiant Consulting Services and Managed Services

Mandiant Consulting Services and Managed Services provide advisory and implementation services (including incident response, strategic readiness, and technical assurance to mitigate threats and reduce incident-related risks) and managed detection and response services and by design, have certain distinct characteristics.

1. Amendments. The Addendum is amended as follows solely with respect to Mandiant Consulting Services and Managed Services:

- The definition of "Data Incident" is supplemented with the following:
    - For clarity, Data Incident excludes incidents that are the subject of the Mandiant Consulting Services and/or Managed Services, as applicable.
- Section 5.2(b)(i) (Compliance with Customer's Instructions) is replaced with the following:

- i. Customer's use of the Services; and

- The second sentence of Section 7.1.1 (Google's Security Measures) is modified to read as follows:
  - The Security Measures may include (as appropriate) measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness.

- Section 7.3.1(b) is modified to read as follows:
  - b. administering, managing access to and securing the account authentication credentials, systems, software, networks and devices that Customer uses to receive, or authorizes Google to access in order to provide, the Mandiant Consulting Services and/or Managed Services, as applicable;

- New Sections 7.3.1(d) and (e) are added as follows:
  - d. minimizing the amount of Customer Data provided by or on behalf of Customer to Google; and
  - e. to the extent Google's access to Customer Data is within Customer's control, revoking that access when Google has completed the Mandiant Consulting Services and/or Managed Services, as applicable.

- Appendix 2 (Security Measures) is replaced with the following:
  - Appendix 2: Additional Technical and Organizational Measures

    1. Customer-Controlled Environment. Google will only access and process Customer Data provided by or on behalf of Customer to Google via a Customer-controlled or Customer-approved account or environment.

    2. Data Access Processes and Policies – Access Policy. Google's data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Customer Data. Google (i) only allows persons to access data they are authorized to access; and (ii) takes steps to ensure that personal data cannot be read, copied, altered or removed without authorization during processing and use. Google's granting or

modification of access rights is based on Customer's provision to Google of end user access to its account or environment.

3. Personnel Security. Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g., certifications). Google's personnel will not process Customer Data without authorization.

4. Additional Security Measures. Google and Customer may agree to additional security measures in the applicable Order Form, including any attached Statement of Work, for the Mandiant Consulting Services and/or Managed Services, as applicable.

2. Customer-Engaged Provider. For clarity, and without limiting Google's obligations under Section 7 (Data Security) or 11 (Subprocessors), Appendix 2 (Security Measures) does not describe the security measures or controls implemented or provided by Customer or Customer-Engaged Providers.

Implementation Services

1. Additional Definitions.

- "*Customer Data*" means data that Customer authorizes Google Personnel to access on Customer-Managed Systems.
- "*Customer-Managed Systems*" means the following, as used by Customer to receive Implementation Services: (a) Customer-managed instances of Google Cloud Services or third-party cloud services; and (b) any hardware or software hosted or managed in Customer's on-premises environment.
- "*Google Cloud Services*" means any Services described in this Appendix 4 (Specific Products), other than Implementation Services, Mandiant Consulting Services and

Mandiant Managed Services.

- "*Google Personnel*" means Google employees and contractors engaged in providing Implementation Services.
- "*Implementation Services*" means advisory, consulting and implementation services provided by Google employees and contractors in support of Google Cloud Services as described in the Agreement, including in an Order Form or a Statement of Work.

2. Amendments. This Addendum is amended as follows with respect to Implementation Services:

- The definition of "Additional Security Controls" is deleted.
- The definition of "Data Incident" is replaced with the following:
  - "*Data Incident*" means a breach of Section 7.1 (Google's Security Measures, Controls and Assistance) by Google Personnel, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.
- Subject to the remainder of this section, the term "Customer Data" is replaced with "Customer Personal Data" when used (a) in Section 2 (Definitions) in the definition of "Subprocessor", and (b) in other sections of this Addendum. For clarity, other definitions in Section 2 (Definitions) remain unamended.
- Section 3 (Duration) is replaced with the following:
  - **3. Duration**. Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, Google no longer has access to any Customer Personal Data.
- Section 6 (Data Deletion) is replaced with the following:
  - **6. Data Deletion.** At the end of the Term, Customer will (a) determine whether to delete any Customer Personal Data, and (b) be responsible for any such deletion.
- The second sentence of Section 7.1.1 (Google's Security Measures) is replaced with the following:

- "The Security Measures may include (as appropriate) measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness."

- Section 7.1.3 (Additional Security Controls) is deleted, together with all other references to that section.

- Section 9.1 (Access; Rectification; Restricted Processing; Portability) is replaced with the following:

  - 9.1 *Access; Rectification; Restricted Processing; Portability*. Customer will be responsible for using the functionality of the Customer-Managed Systems to access, rectify and restrict processing of Customer Personal Data, including if Customer becomes aware that any Customer Personal Data is inaccurate or outdated and is required by Applicable Privacy Law to rectify or delete that data.

- Section 11.4 (Opportunity to Object to Subprocessors) is replaced with the following:

  - 11.4 *Opportunity to Object to Subprocessors*. When any New Subprocessor is engaged during the Term, Google will notify Customer of the engagement of the New Subprocessor before it processes Customer Personal Data. Customer may object to the New Subprocessor by notifying Google and, if Customer does so, the parties will work in good faith to determine a mutually acceptable alternative.

- Appendix 1 (Subject Matter and Details of Data Processing) is amended as follows:

  - The "Duration of the Processing" section is replaced with the following:

    - *"Duration of the Processing*. The Term plus (if applicable) the period from the end of the Term until the expiry of Google's access to any Customer Personal Data."

  - The words "provided to Google via the Services" in the "Categories of Data" and "Data Subjects" sections are replaced with "made accessible to Google in connection with the Services".

- Appendix 2 (Security Measures) is replaced with the following:

  - **Appendix 2: Security Measures**

1. Customer-Managed Systems. Google Personnel will only access and process Customer Personal Data on Customer-Managed Systems. If those systems include Google Cloud Services, Customer's use of Google Cloud Services remains governed by the agreement applicable to those services.

2. Access Control. Google's internal data access processes and policies are designed to prevent unauthorized persons and systems from gaining access to Google Cloud Services used to process personal data. Google policies (i) only allow Google Personnel to access data they are authorized to access; and (ii) require that Google Personnel do not read, copy, alter or remove Customer Personal Data without authorization during processing, use and after recording. Customer controls the provisioning or modification of end user access rights to Customer-Managed Systems. If those systems include Google Cloud Services, details regarding workflow tools that maintain audit records of changes and system access logs are addressed in the agreement for the applicable Google Cloud Services.

3. Personnel Security. Google Personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Google Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Google Personnel are provided with security training. Google Personnel handling Customer Personal Data are required to complete additional requirements appropriate to their role (e.g., certifications).

4. Additional Security Measures. Google and Customer may agree to additional security measures in the Agreement, including in an Order Form or a Statement of Work.

5. Subprocessor Security. Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are

engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement), the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

3. Customer Security Responsibilities. In addition to its obligations under Section 7.3.1 (Customer's Security Responsibilities), Customer is responsible for the following:

- administering, managing access to, and securing Customer-Managed Systems, including minimizing Google Personnel's access to Customer Personal Data to the extent reasonably practicable and terminating that access on completion of the Implementation Services; and
- implementing any security recommendations provided in writing by Google to Customer with respect to Customer-Managed Systems.

4. Compliance Certification. Google will maintain certificates for ISO 27001, ISO 27017 and ISO 27018 covering Implementation Services provided in support of Google Cloud Platform and Google Workspace (the "*Implementation Services Compliance Certifications*"). Google may add standards at any time. Google may replace an Implementation Services Compliance Certification with an equivalent or enhanced alternative.

5. Reviews of Compliance Certification. To demonstrate compliance by Google with its obligations under this Addendum, Google will make the Implementation Services Compliance Certification available for review by Customer and, if Customer is a processor, allow Customer to request access for the relevant controller to the Implementation Services Compliance Certification.

6. Data Processing Locations. Customer Personal Data may be processed in any country where Google provides Implementation Services or where Customer maintains Customer-Managed Systems.

7. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for Implementation Services.

8. Information about Subprocessors. Subprocessors for Implementation Services will be identified (as subcontractors) in an applicable Order Form, Statement of Work, or other confirmation provided to Customer before commencement of the Implementation Services or will be Google Affiliates. Google will also make names, locations and activities of Subprocessors for Implementation Services available to Customer upon request.

9. Google's Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

Google Cloud Skills Boost for Organizations

1. Additional Definitions.

- "*Account*", if not defined in the Agreement, means Customer's Google Cloud Skills Boost for Organizations Customer Account.
- "*GCSBO*" means educational, training, and learning services and content provided through https://www.cloudskillsboost.google/ (https://www.cloudskillsboost.google/) (or another website operated or controlled by Google and used for purposes of Google Cloud Skills Boost for Organizations).
- "*TSS*" means technical support services that Google, in its discretion, may provide to Customer.

2. Amendments. This Addendum is amended as follows with respect to GCSBO:

- The definition of "Additional Security Controls" is replaced with the following:
    - *"Additional Security Controls"* means security resources, features, functionality and/or controls (if any) that Customer may use at its option and/or as it determines, including (if any) encryption, logging and monitoring, identity and access management, and security scanning.
- The definitions of "SCCs (Controller-to-Processor)", "SCCs (Processor-to-Controller)", "SCCs (Processor-to-Processor)" and "SCCs (Processor-to-Processor, Google Exporter)" in Appendix 3 (Specific Privacy Laws) are replaced with the following:

- "SCCs (Controller-to-Processor)" means the terms at: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-c2p (https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-c2p);
- "SCCs (Processor-to-Controller)" means the terms at: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2c (https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2c);
- "SCCs (Processor-to-Processor)" means the terms at: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p (https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p); and
- "SCCs (Processor-to-Processor, Google Exporter)" means the terms at: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p-intra-group (https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p-intra-group).

3. Data Center Locations. The locations of GCSBO data centers are described at https://cloud.google.com/about/locations/ (https://cloud.google.com/about/locations/).

4. No Certification by Non-EMEA Customers. Customer is not obliged to certify or identify its competent Supervisory Authority as described in Section 4.2 (Certification by Non-EMEA Customers) of the European Data Protection terms in Appendix 3 (Specific Privacy Laws) for GCSBO.

5. Information about Subprocessors. Names, locations, and activities of GCSBO Subprocessors are described at:

a. https://cloud.google.com/terms/skillsboost-organizations/subprocessors (https://cloud.google.com/terms/skillsboost-organizations/subprocessors); and

b. https://cloud.google.com/terms/subprocessors (https://cloud.google.com/terms/secops/subprocessors).

6. Cloud Data Protection Team. The Data Protection Team for GCSBO can be contacted at https://support.google.com/qwiklabs (https://support.google.com/qwiklabs) (and/or via such other means as Google may provide from time to time).

7. Google's Processing Records. To the extent any Applicable Privacy Law requires Google to collect and maintain records of certain information relating to Customer, Customer will supply such information to Google upon request, and notify Google of any

updates required to keep such information accurate and up-to-date, unless Google requests that Customer supply and update such information via another means.

Previous versions of Data Processing and Security Terms:

April 9, 2024 (/terms/data-processing-addendum/index-20240409) *June 30, 2022* (/terms/data-processing-addendum/index-20220630) *September 24, 2021* (/terms/data-processing-terms/index-20210924) *August 19, 2020* (/terms/data-processing-terms/index-20200819) *August 10, 2020* (https://cloud.google.com/terms/data-processing-terms-20200810) *July 17, 2020* (https://cloud.google.com/terms/data-processing-terms-20200717) *October 11, 2019* (https://cloud.google.com/terms/data-processing-terms-20191011) *October 1, 2019* (https://cloud.google.com/terms/data-processing-terms-20191001) (https://cloud.google.com/terms/data-processing-terms-20180525) *May 25, 2018* (https://cloud.google.com/terms/data-processing-terms-20180525) *March 13, 2018* (https://cloud.google.com/terms/data-processing-terms-20180313) *November 9, 2017* (https://cloud.google.com/terms/data-processing-terms-20171109) *October 11, 2017* (https://cloud.google.com/terms/data-processing-terms-20171011) *February 7, 2017* (https://cloud.google.com/terms/data-processing-terms-20170207) *October 6, 2016* (https://cloud.google.com/terms/data-processing-terms-20161006)

Previous versions of Data Processing Amendment:

July 7, 2022 (https://workspace.google.com/terms/07072022/dpa_terms.html) *September 24, 2021* (https://workspace.google.com/terms/09242021/dpa_terms.html) *May 27, 2021* (https://workspace.google.com/terms/05272021/dpa_terms.html) *October 29, 2019* (https://workspace.google.com/terms/10292019/dpa_terms.html) *May 25, 2018* (https://workspace.google.com/terms/05252018/dpa_terms.html) *April 25, 2018* (https://workspace.google.com/terms/04252018/dpa_terms.html) *July 11, 2017* (https://workspace.google.com/terms/07112017/dpa_terms.html) *November 28, 2016* (https://workspace.google.com/terms/11282016/dpa_terms.html) *January 7, 2016* (https://workspace.google.com/terms/01072016/dpa_terms.html) *April 24, 2015* (https://workspace.google.com/terms/04242015/dpa_terms.html) *April 1, 2014* (https://workspace.google.com/terms/04012014/dpa_terms.html) *November 14, 2012* (https://workspace.google.com/terms/11142012/dpa_terms.html)

Previous versions of Data Processing Addendum for Looker (original) Services (Customers):

February 14, 2023 (https://cloud.google.com/terms/looker/dpst/index-20230214)*January 4, 2023* (https://cloud.google.com/terms/looker/dpst/index-20230104)*September 20, 2022* (https://cloud.google.com/terms/looker/dpst/dpst-20220920)*June 30, 2022* (https://cloud.google.com/terms/looker/dpst/dpst-20220630)*March 16, 2022* (https://cloud.google.com/terms/looker/dpst/dpst-20220316)*September 24, 2021* (https://cloud.google.com/terms/looker/dpst/dpst-20210924)*April 1, 2021* (https://cloud.google.com/terms/looker/dpst/dpst-20210401)*January 15, 2021* (https://cloud.google.com/terms/looker/dpst/dpst-20210115)*December 17, 2020* (https://cloud.google.com/terms/looker/dpst/dpst-20201217)*August 28, 2020* (https://cloud.google.com/terms/looker/dpst/dpst-20200828)*June 1, 2020* (https://cloud.google.com/terms/looker/dpst/dpst-20200601)*March 9, 2020* (https://cloud.google.com/terms/looker/dpst/dpst-20200309) (https://cloud.google.com/terms/looker/dpst/index-20230214)

Previous versions of SecOps Services DPST (Customers):

February 6, 2023 (/terms/secops/data-processing-terms/index-20230206) November 28, 2022 (/terms/secops/data-processing-terms/index-20221128) September 27, 2021 (/terms/secops/data-processing-terms/index-20210927) October 1, 2020 (/terms/secops/data-processing-terms/index-20201001)

Previous versions of Data Processing Addendum for SecOps Consulting Services and Managed Services:

October 5, 2023 (/terms/secops/data-processing-addendum/index-20231005) September 19, 2023 (/terms/secops/data-processing-addendum/index-20230919) June 15, 2023 (/terms/secops/data-processing-addendum/index-20230615) February 22, 2023 (/terms/secops/data-processing-addendum/index-20230222) February 6, 2023 (https://cloud.google.com/terms/secops/data-processing-addendum/index-20230206)

PREVIOUS VERSIONS *(Last modified October 15, 2024)*

September 26, 2024 (https://cloud.google.com/archive/terms/data-processing-addendum-20240926)

September 9, 2024 (/legal/archive/terms/data-processing-addendum/index-20240909)

August 5, 2024 _ (/legal/archive/terms/data-processing-addendum/index-20240805)

May 23, 2024 _ (/terms/data-processing-addendum/index-20240523) April 9, 2024 (/terms/data-processing-addendum/index-20240409) November 8, 2023 (/terms/data-processing-addendum/index-20231108) August 15, 2023 (/terms/data-processing-addendum/index-20230815) September 20, 2022 (/terms/data-processing-addendum/index-20220920)